

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 4 月 8 日 (08.04.2004)

PCT

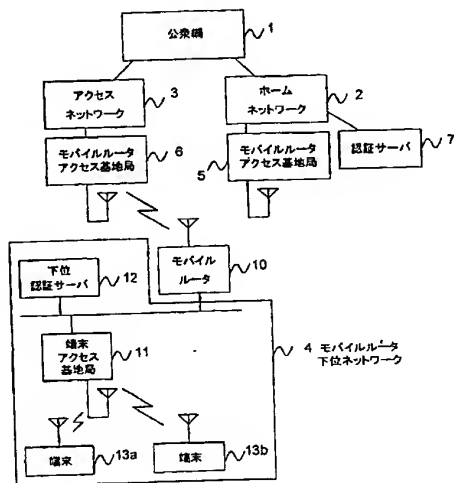
(10) 国際公開番号
WO 2004/029819 A1

- (51) 国際特許分類⁷: G06F 15/00, H04B 7/26, H04L 12/28
- (21) 国際出願番号: PCT/JP2003/012318
- (22) 国際出願日: 2003 年 9 月 26 日 (26.09.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-284334 2002 年 9 月 27 日 (27.09.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真 1 0 0 6 番地 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 田中 武志

- (74) 代理人: 二瓶 正敬 (NIHEI, Masayuki); 〒160-0004 東京都 新宿区 四谷 2 丁目 1 2-5 第 6 富沢ビル 6 F Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, [続葉有]

(54) Title: TERMINAL AUTHENTICATION SYSTEM, TERMINAL AUTHENTICATION METHOD, AND TERMINAL AUTHENTICATION SERVER

(54) 発明の名称: 端末認証システム及び端末認証方法並びに端末認証サーバ



- 1...PUBLIC NETWORK
3...ACCESS NETWORK
6...MOBILE ROUTER ACCESS BASE STATION
2...HOME NETWORK
5...MOBILE ROUTER ACCESS BASE STATION
7...AUTHENTICATION SERVER
12...LOWER NODE AUTHENTICATION SERVER
10...MOBILE ROUTER
11...TERMINAL ACCESS BASE STATION
13a...TERMINAL
13b...TERMINAL
4...MOBILE ROUTER LOWER NODE NETWORK

(57) Abstract: It is possible to effectively authenticate a terminal which attempts connection to (participation in) a mobile network even when the connection between a mobile router and a ground side mobile router access base station is unstable or disabled. In addition to a first authentication server (authentication server (7)) arranged at a position apart from a mobile network (mobile router lower node network (4)) arranged in a mobile body, a second authentication server (lower node authentication server (12)) is arranged in the mobile network so that authentication of mobile terminals (terminals 13a, 13b) can also be performed in the second authentication server. Especially when the connection between the mobile network of the mobile body side and the first authentication server of the ground side (that is, communication between a mobile router 10 and mobile router access base stations 5, 6) is disabled, the second authentication server authenticates a mobile terminal which attempts to participate in the mobile network.

(57) 要約: 移動するモバイルルータと地上側のモバイルルータアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続(参加)を試みている端末の認証を効率良く行うことを目的とし、移動体内に配置されている移動ネットワーク(モバイルルータ下位ネットワーク4)から離れた場所に配置された第1認証サーバ(認証サーバ7)とは別に、第2認証サーバ(下位認証サーバ12)を移動ネットワーク内に配置し、第2認証サーバにおいても移動端末(端末13a、13b)の認証が行えるようにする。特に、移動体側の移動ネットワークと地上側の第1認証サーバとの間の接続(すなわち、モバイルルータ10とモバイルルータアクセス基地局5、6間との通信)が不可能となった場合に、第2認証サーバが、移動ネットワークへの参加を試みる移動端末の認証を行うようにする。



SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, YU, ZA, ZM, ZW.

OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ,
SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM,
AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許
(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,
GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR),

添付公開書類:

— 国際調査報告書

2 文字コード及び他の略語については、定期発行される
各 PCT ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

明 細 書

端末認証システム及び端末認証方法並びに端末認証サーバ

5 技術分野

本発明は、移動体内に配置されている移動ネットワークに移動端末が参加する際に認証処理を行う端末認証システム及び端末認証方法並びに端末認証サーバに関する。

10 背景技術

従来、端末がモバイルルータ下位ネットワーク（移動体内に配置される移動ネットワーク）への接続（参加）を行おうとする場合、その端末の接続の可否を決める認証処理は、移動可能なモバイルルータ下位ネットワークとは異なる地上側のホームネットワークに属する認証サーバで行われている。認証サーバは、端末から利用者名やパスワードなどの認証に必要となる認証データを受け、この認証データを参照し、当該端末に対して、モバイルルータ下位ネットワークへの接続の許可／不許可を決定する認証処理を行っている。

また、例えば、（特許文献1）には、所定の端末の認証情報を有するLAN（Local Area Network：ローカルエリアネットワーク）とは異なるLANに当該所定の端末が接続しようとした場合、所定の端末が接続を試みているLANの認証サーバが、所定の端末の認証情報を有するLANの認証サーバに対して、所定の端末の認証を依頼し、所定の端末がLANに接続する権利を有しているか否かを判断する方法が開示されている。

特許文献1 特開平10-70540号公報（段落[0014]～[

0067]、図1、図2、図5)

しかしながら、モバイルルータは移動可能であり、かつ、アクセス基地局と無線通信によって接続する。したがって、モバイルルータとアクセス基地局との間の接続は不安定であり、一時的に接続が利用できなくなってしまうことが頻繁に起きる。このように、接続が利用不可能とな
5 ってしまった状態では、モバイルルータ下位ネットワーク（移動ネットワーク）は、ホームネットワーク上の認証サーバに対して、端末の認証を依頼することができず、端末の認証は不可能となってしまう。したがって、モバイルルータ下位ネットワークへの接続を試みている端末は、
10 モバイルルータがアクセス基地局と接続できるようになるまでの間、モバイルルータ下位ネットワークへの接続（参加）ができないという問題がある。また、モバイルルータ下位ネットワークが移動し、ホームネットワークから離れた場合には、モバイルルータ下位ネットワークとホームネットワーク上の認証サーバとの距離は広がり、認証における時間や
15 トラフィックなどが増大してしまうという問題がある。

発明の開示

上記課題を解決するため、本発明では、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、モバイルルータ下位ネットワークへの接続（参加）を試みている端末の認証を
20 効率良く行うことを可能とする端末認証システム及び端末認証方法並びに端末認証サーバを提供することを目的とする。

上記目的を達成するため、本発明の端末認証システムでは、移動体内に配置されている移動ネットワーク（モバイルルータ下位ネットワーク）から離れた場所に配置された第1認証サーバ（認証サーバ）とは別に、
25 第2認証サーバ（下位認証サーバ）を移動ネットワーク内に配置し、第

2 認証サーバにおいても移動端末（端末）の認証が行えるよう構成されている。

この構成により、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（
5 参加）を試みている端末の認証を効率良く行うことが可能となる。

さらに、本発明の端末認証システムでは、第2認証サーバが、移動端末の認証を行うことを可能とする認証手段と、移動端末の認証時に参照する認証データを格納することが可能な情報格納手段とを有している。

この構成により、移動ネットワークに属し、移動体と共に移動する第
10 2認証サーバで確実に認証処理を行うことが可能となる。

さらに、本発明の端末認証システムでは、移動端末から第2認証サーバに対して、認証要求が送信されるよう構成されている。

この構成により、第2認証サーバが、移動ネットワークへの参加を試みている移動端末の存在を確実に認識できるようになる。

15 さらに、本発明の端末認証システムでは、第2認証サーバが、第1認証サーバと第2認証サーバとの通信が可能か否かを判断する接続判断手段を有し、第2認証サーバが移動端末から認証要求を受けた場合、第1認証サーバとの通信が可能と判断された場合には第1認証サーバに認証要求を送って第1認証サーバから移動端末の認証結果を受信し、第1認
20 証サーバとの通信が不可能と判断された場合には認証手段を用いて移動端末の認証を行うよう構成されている。

この構成により、第1認証サーバにおける認証が可能な場合には、第1認証サーバで認証を行い、第1認証サーバでの認証が不可能な場合のみ、第2認証サーバで認証を行うようにすることが可能となる。

25 さらに、本発明の端末認証システムでは、第1認証サーバに認証要求を送って第1認証サーバから移動端末の認証結果を受信した場合、第2

認証サーバは、移動端末の識別情報と移動端末の認証結果とを関連付けて、情報格納手段に認証データとして格納するよう構成されている。

この構成により、第2認証サーバは、第1認証サーバで認証に成功した移動端末を把握することが可能となり、次回以降、当該移動端末の認

5 証を第2認証サーバで行えるようになる。

さらに、本発明の端末認証システムでは、第2認証サーバが、第1認証サーバと第2認証サーバとの通信が可能か否かを判断する接続判断手段を有し、接続判断手段が第1認証サーバとの通信が可能か否かを判断し、第1認証サーバとの通信が可能と判断された場合、第2認証サーバ
10 は、任意のタイミングで第1認証サーバから移動端末の認証に必要な認証データを取得し、情報格納手段に格納するよう構成されている。

この構成により、第2認証サーバは、第1認証サーバとの通信が可能な状態のときに、端末の認証に必要な情報をあらかじめ第1認証サーバから取得できるようになる。

15 さらに、本発明の端末認証システムでは、第2認証サーバは、所定のタイミングで第1認証サーバから認証データを取得し、情報格納手段に格納されている認証データを更新するよう構成されている。

この構成により、第2認証サーバは、第1認証サーバとの同期を図ることが可能となり、第2認証サーバは、常に第1認証サーバが格納する
20 最新の情報を取得することが可能となる。

さらに、本発明の端末認証システムでは、第2認証サーバで移動端末の認証を行って移動端末の認証に失敗した場合、第2認証サーバは、第1認証サーバに認証要求を送って第1認証サーバから移動端末の認証結果を受信するよう構成されている。

25 この構成により、なるべく第2認証サーバで認証を行い、認証に失敗した場合のみ第1認証サーバで、確実な認証処理を再度行うことによ

て、時間やトラフィックの削減を図ることが可能となる。

さらに、本発明の端末認証システムでは、第2認証サーバから認証要求を送信した移動端末に対して、第1認証サーバ又は第2認証サーバで行われた認証結果が通知されるよう構成されている。

- 5 この構成により、第1認証サーバ又は第2認証サーバで行われた認証結果が、第2認証サーバから移動端末に対して通知されるようにすることが可能となり、第2認証サーバが、すべての端末の認証結果を把握できるようになる。

- 10 また、上記目的を達成するため、本発明の端末認証方法では、移動体内に配置されている移動ネットワークに移動端末が参加する場合、移動ネットワークから離れた場所に配置された第1認証サーバとは別に、移動ネットワーク内に配置された第2認証サーバが、移動端末の認証を行うようにしている。

- 15 これにより、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことが可能となる。

さらに、本発明の端末認証方法では、移動端末が、第2認証サーバに対して、認証要求を送信するようにしている。

- 20 これにより、第2認証サーバが、移動ネットワークへの参加を試みている移動端末の存在を確実に認識できるようになる。

- さらに、本発明の端末認証方法では、第2認証サーバが移動端末から認証要求を受けた場合、第1認証サーバと第2認証サーバとの通信が可能か否かを判断し、第1認証サーバとの通信が可能と判断された場合には第1認証サーバに認証要求を送って第1認証サーバから移動端末の認証結果を受信し、第1認証サーバとの通信が不可能と判断された場合には第2認証サーバが移動端末の認証を行うようにしている。
- 25

これにより、第1認証サーバにおける認証が可能な場合には、第1認証サーバで認証を行い、第1認証サーバでの認証が不可能な場合のみ、第2認証サーバで認証を行うようにすることが可能となる。

さらに、本発明の端末認証方法では、第1認証サーバに認証要求を送
5 って第1認証サーバから移動端末の認証結果を受信した場合、第2認証サーバは、移動端末の識別情報と移動端末の認証結果とを関連付けて格納するようにしている。

これにより、第2認証サーバは、第1認証サーバで認証に成功した移動端末を把握することが可能となり、次回以降、当該移動端末の認証を
10 第2認証サーバで行えるようになる。

さらに、本発明の端末認証方法では、第2認証サーバが、第1認証サーバと第2認証サーバとの通信が可能か否かを判断し、第1認証サーバとの通信が可能と判断された場合には、任意のタイミングで第1認証サーバから移動端末の認証に必要な認証データを取得し格納するよう
15 にしている。

これにより、第2認証サーバは、第1認証サーバとの通信が可能な状態のときに、端末の認証に必要な情報をあらかじめ第1認証サーバから取得できるようになる。

さらに、本発明の端末認証方法では、第2認証サーバが、所定のタイ
20 ミングで第1認証サーバから認証データを取得し、第2認証サーバに格納されている認証データを更新するようにしている。

これにより、第1認証サーバで、確実な認証処理を再度行うことによって、時間やトラフィックの削減を図ることが可能となる。

さらに、本発明の端末認証方法では、第2認証サーバが、認証要求を
25 送信した移動端末に対して、第1認証サーバ又は第2認証サーバで行われた認証結果を通知するようにしている。

これにより、第1認証サーバ又は第2認証サーバで行われた認証結果が、第2認証サーバから移動端末に対して通知されるようにすることが可能となり、第2認証サーバが、すべての端末の認証結果を把握できるようになる。

- 5 また、上記目的を達成するため、本発明の端末認証サーバは、移動体内に配置されている移動ネットワークに移動端末が参加する場合、移動端末の認証を行うことが可能な端末認証サーバであり、移動ネットワークから離れた場所に配置された端末認証サーバとは別に、移動ネットワーク内に配置されるよう構成されている。

- 10 この構成により、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことが可能となる。

さらに、本発明の端末認証サーバでは、移動端末の認証を行うことを可能とする認証手段と、移動端末の認証時に参照する認証データを格納

- 15 することが可能な情報格納手段とを有している。

この構成により、移動ネットワークに属し、移動体と共に移動する端末認証サーバで確実に認証処理を行うことが可能となる。

さらに、本発明の端末認証サーバでは、移動端末から認証要求を受信するよう構成されている。

- 20 この構成により、移動ネットワーク内の端末認証サーバが、移動ネットワークへの参加を試みている移動端末の存在を確実に認識できるようになる。

さらに、本発明の端末認証サーバでは、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続

- 25 判断手段を有し、移動端末から認証要求を受けた場合、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能と判断さ

れた場合には、移動ネットワークから離れた場所に配置された端末認証サーバに認証要求を送って、移動ネットワークから離れた場所に配置された端末認証サーバから移動端末の認証結果を受信し、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が不可能と判断
5 された場合には、認証手段を用いて移動端末の認証を行うよう構成されている。

この構成により、ホームネットワークに属する端末認証サーバにおける認証が可能な場合には、ホームネットワークに属する端末認証サーバで認証を行い、ホームネットワークに属する端末認証サーバでの認証が
10 不可能な場合のみ、移動ネットワーク内の端末認証サーバで認証を行うようにすることが可能となる。

さらに、本発明の端末認証サーバでは、移動ネットワークから離れた場所に配置された端末認証サーバから移動端末の認証結果を受信した場合、移動端末の識別情報と移動端末の認証結果とを関連付けて、情報格
15 納手段に認証データとして格納するよう構成されている。

この構成により、移動ネットワーク内の端末認証サーバは、ホームネットワークに属する端末認証サーバで認証に成功した移動端末を把握することが可能となり、次回以降、当該移動端末の認証を移動ネットワーク内の端末認証サーバで行えるようになる。

さらに、本発明の端末認証サーバでは、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続
20 判断手段を有し、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能と判断された場合、任意のタイミングで、移動ネットワークから離れた場所に配置された端末認証サーバから移動端末
25 の認証に必要な認証データを取得し、情報格納手段に格納する構成されている。

この構成により、移動ネットワーク内の端末認証サーバは、ホームネットワークに属する端末認証サーバとの通信が可能な状態のときに、端末の認証に必要な情報をあらかじめホームネットワークに属する端末認証サーバから取得できるようになる。

- 5 さらに、本発明の端末認証サーバでは、所定のタイミングで、移動ネットワークから離れた場所に配置された端末認証サーバから認証データを取得し、情報格納手段に格納されている前記認証データを更新するよう構成されている。

- 10 この構成により、移動ネットワーク内の端末認証サーバは、ホームネットワークに属する端末認証サーバとの同期を図ることが可能となり、移動ネットワーク内の端末認証サーバは、常にホームネットワークに属する端末認証サーバが格納する最新の情報を取得することが可能となる。

- 15 さらに、本発明の端末認証サーバでは、認証手段により移動端末の認証を行って、移動端末の認証に失敗した場合、移動ネットワークから離れた場所に配置された端末認証サーバに認証要求を送って端末認証サーバから移動端末の認証結果を受信するよう構成されている。

- 20 この構成により、なるべく移動ネットワーク内の端末認証サーバで認証を行い、認証に失敗した場合のみホームネットワークに属する端末認証サーバで、確実な認証処理を再度行うことによって、時間やトラフィックの削減を図ることが可能となる。

さらに、本発明の端末認証サーバでは、認証要求を送信した移動端末に対して、移動ネットワークから離れた場所に配置された端末認証サーバ、又は、当該端末認証サーバで行われた認証結果を通知するよう構成されている。

- 25 この構成により、ホームネットワークに属する端末認証サーバ又は移動ネットワーク内の端末認証サーバで行われた認証結果が、移動ネット

ワーク内の端末認証サーバから移動端末に対して通知されるようにすることが可能となり、移動ネットワーク内の端末認証サーバが、すべての端末の認証結果を把握できるようになる。

5 図面の簡単な説明

図 1 は、本発明の実施の形態を示すネットワーク構成図、

図 2 は、本発明の実施の形態のネットワークに配置されている端末の内部構成を示すブロック図、

図 3 は、本発明の実施の形態のネットワークに配置されているモバイルルータの内部構成を示すブロック図、

図 4 は、本発明の実施の形態のネットワークに配置されている下位認証サーバの内部構成を示すブロック図、

図 5 は、図 4 に示す下位認証サーバの動作を説明するためのフローチャート、

図 6 は、本発明の実施の形態のネットワークに配置されている下位認証サーバの内部構成の別の一例を示すブロック図である。

発明を実施するための最良の形態

以下、図面を参照しながら、本発明の実施の形態について説明する。

図 1 は、本発明の実施の形態を示すネットワーク構成図である。図 1 に示すネットワークは、公衆網 1、ホームネットワーク 2、アクセスネットワーク 3、モバイルルータ下位ネットワーク 4、ホームネットワーク 2 と接続するモバイルルータアクセス基地局 5、アクセスネットワーク 3 と接続するモバイルルータアクセス基地局 6、ホームネットワーク 2 に接続する認証サーバ 7、モバイルルータ下位ネットワーク 4 と接続するモバイルルータ 10 により構成される。

モバイルルータ下位ネットワーク 4 は、例えば、移動可能な乗り物などの移動体内に配置されているものであり、モバイルルータ 10 を介してモバイルルータアクセス基地局 5、6 と無線通信による接続が可能である。すなわち、モバイルルータ 10 とモバイルルータアクセス基地局 5 とが無線通信によって接続している場合には、モバイルルータ下位ネットワーク 4 は、モバイルルータ 10、モバイルルータアクセス基地局 5、ホームネットワーク 2 を経由して、公衆網 1 と接続可能とであり、モバイルルータ 10 とモバイルルータアクセス基地局 6 とが無線通信によって接続している場合には、モバイルルータ下位ネットワーク 4 は、モバイルルータ 10、モバイルルータアクセス基地局 6、アクセスネットワーク 3 を経由して、公衆網 1 と接続可能である。なお、図 1 において、アクセスネットワーク 3、モバイルルータアクセス基地局 5、6 はそれぞれ 1 つずつ図示されているが、複数配置することも可能である。

また、モバイルルータ下位ネットワーク 4 は、端末アクセス基地局 11、モバイルルータ下位ネットワーク 4 上の下位認証サーバ 12、複数の端末 13（図 1 では、端末 13 a、13 b の 2 つの端末 13 が図示されている）により構成されている。端末アクセス基地局 11、モバイルルータ下位ネットワーク 4 上の下位認証サーバ 12 は、モバイルルータ 10 と接続されており、また、端末 13 は、端末アクセス基地局 11 との無線通信を介して、モバイルルータ 10 や下位認証サーバ 12 への接続が可能であり、さらには、モバイルルータ 10 からホームネットワーク 2 やアクセスネットワーク 3 を経由して、公衆網 1 への接続が可能である。

モバイルルータ 10 及びモバイルルータ下位ネットワーク 4 は、本来ホームネットワーク 2 に所属し、管理されており、端末 13 がモバイルルータ下位ネットワーク 4 に接続する権利を有するか否かの確認（認証

）は、認証サーバ 7 によって行われる。また、認証サーバ 7 には、この認証処理を行うための認証データ（利用者名やパスワードなど）が格納されている。

- 次に、図 1 に示す端末 1 3 の内部構成の一例について説明する。図 2 は、本発明の実施の形態のネットワークに配置されている端末の内部構成を示すブロック図である。なお、図 1 に示されている端末 1 3 は、図 2 に示す内部構成を有している。図 2 に示す端末 1 3 は、無線通信手段 2 0、通信制御手段 2 1、送信手段 2 2、受信手段 2 3、情報格納手段 2 4、入出力制御手段 2 5、入出力手段 2 6 により構成される。
- 無線通信手段 2 0 及び通信制御手段 2 1 は、端末アクセス基地局 1 1 などの端末 1 3 外部の通信装置との通信を行うことを可能とするものである。無線通信手段 2 0 がデータを受信した場合、その受信データは、通信制御手段 2 1 を経由して受信手段 2 3 に供給され、さらに、受信データは、受信手段 2 3 から情報格納手段 2 4 や入出力制御手段 2 5 に供給可能なようになっている。また、情報格納手段 2 4 には、MAC アドレスなどの端末 ID や認証データが格納されており、例えば、認証サーバ 7 や下位認証サーバ 1 2 に認証要求を送信する場合、送信手段 2 2 は、通信制御手段 2 1 及び無線通信手段 2 0 を通じて、これらの端末 ID や認証データを外部に送信することが可能である。また、入出力制御手段 2 5 及び入出力手段 2 6 は、入力データの送信や受信データの出力を可能とするものであり、認証に成功して、端末 1 3 がモバイルルータ下位ネットワーク 4 に接続可能となった場合には、主に、入出力制御手段 2 5 及び入出力手段 2 6 を介して、通信データの送受信が行われる。

- 次に、図 1 に示すモバイルルータ 1 0 の内部構成の一例について説明する。図 3 は、本発明の実施の形態のネットワークに配置されているモバイルルータの内部構成を示すブロック図である。なお、図 1 に示され

ているモバイルルータ 10 は、図 3 に示す内部構成を有している。図 3 に示すモバイルルータ 10 は、ローカル通信手段 31、ローカル通信制御手段 32、外部接続検知結果送信手段 33、外部接続検知手段 34、通信制御手段 35、無線通信手段 36、経路制御手段 37 により構成される。

無線通信手段 36 及び通信制御手段 35 は、モバイルルータアクセス基地局 5、6 などのモバイルルータ 10 外部の通信装置との通信を行うことを可能とするものである。また、外部接続検知手段 34 は、無線通信手段 36 がモバイルルータ 10 外部との無線接続が利用可能かを検知し、その外部接続検知結果を経路制御手段 37 及び外部接続検知結果送信手段 33 に伝達するものである。

外部接続検知結果送信手段 33 は、ローカル通信制御手段 32 を介してローカル通信手段 31 と接続し、外部接続検知結果を LAN 30 上に出力する。この LAN 30 には、端末アクセス基地局 11 や下位認証サーバ 12 が接続しており、外部接続検知結果送信手段 33 から下位認証サーバ 12 に対して、外部接続検知結果を伝達することが可能である。

また、ローカル通信制御手段 32 は、ローカル通信手段 31 を介して、LAN 30 に接続する端末アクセス基地局 11 や下位認証サーバ 12、さらには、端末アクセス基地局 11 に接続する端末 13 から、モバイルルータ下位ネットワーク 4 外部への送信データを受信することが可能である。経路制御手段 37 は、ローカル通信制御手段 32 が受信した当該送信データに対して適切に経路制御を行い、経路制御された当該送信データは、通信制御手段 35 及び無線通信手段 36 を介してモバイルルータ 10 外部の通信装置に無線通信によって伝送される。また、無線通信手段 36 及び通信制御手段 35 を介してモバイルルータ下位ネットワーク 4 外部から受信した受信データに関しても、同様に経路制御手段 37

が適切に経路制御を行い、ローカル通信制御手段 3 2 及びローカル通信手段 3 1 を介して LAN 3 0 上に伝送される。

次に、図 1 に示す下位認証サーバ 1 2 の内部構成の一例について説明する。図 4 は、本発明の実施の形態のネットワークに配置されている下
5 位認証サーバの内部構成を示すブロック図である。なお、図 1 に示されている下位認証サーバ 1 2 は、図 4 に示す内部構成を有している。図 4 に示す下位認証サーバ 1 2 は、ローカル通信手段 4 1、ローカル通信制御手段 4 2、外部接続検知結果受信手段 4 3、認証要求受付手段 4 4、
10 認証依頼送信手段 4 5、認証結果受信手段 4 6、認証結果送信手段 4 7、認証データ比較手段 4 8、情報格納手段 4 9 により構成される。

また、図 5 は、図 4 に示す下位認証サーバの動作を説明するためのフローチャートである。以下、図 5 を参照しながら下位認証サーバ 1 2 の動作について説明する。まず、下位認証サーバ 1 2 は、移動ネットワークに参加しようとしている端末 1 3 から、当該端末 1 3 の端末 ID 及び
15 この端末 1 3 の利用者とパスワードを含む認証データを認証要求として受信する（ステップ S 2）。一方で、下位認証サーバ 1 2 は、LAN 3 0 を経由してモバイルルータ 1 0 から送信されてくる外部接続検知結果を、ローカル通信手段 4 1 及びローカル通信制御手段 4 2 を介して、
20 外部接続検知結果受信手段 4 3 により受信する（ステップ S 3）。なお、下位認証サーバ 1 2 は、端末 1 3 から認証要求を受けた場合にのみ、モバイルルータ 1 0 に対して外部接続検知結果を要求するようにすることも可能であり、また、定期的にモバイルルータ 1 0 から外部接続検知結果の取得を行うようにすることも可能である。

外部接続検知結果受信手段 4 3 によって受信された外部接続検知結果
25 は、認証要求受付手段 4 4 に供給され、外部接続が利用可能か否か（すなわち、認証サーバ 7 との通信が可能か否か）が判断される（ステップ

S 4)。外部接続が利用可能な場合には、認証要求と共に端末 1 3 から受信した認証データを情報格納手段 4 9 内の「利用者の認証データ」テーブルに格納し（ステップ S 5）、認証要求受付手段 4 4 から認証依頼送信手段 4 5 に認証要求を供給する。

- 5 認証依頼送信手段 4 5 は、ローカル通信制御手段 4 2 及びローカル通信手段 4 1、LAN 3 0、モバイルルータ 1 0 を介して（モバイルルータ 1 0 が、アクセスネットワーク 3 に接続するモバイルルータアクセス基地局 6 と通信を行っている場合には、さらに、アクセスネットワーク 3 及び公衆網 1 を介して）、ホームネットワーク 2 上の認証サーバ 7 に対して、当該認証要求を送信し（ステップ S 6）、認証サーバ 7 における認証を依頼する。

- 15 認証サーバ 7 では、当該認証要求に係る認証が行われ、下位認証サーバ 1 2 は、その認証結果を LAN 3 0、ローカル通信手段 4 1 及びローカル通信制御手段 4 2 を介して、認証結果受信手段 4 6 によって受信する（ステップ S 7）。そして、認証結果受信手段 4 6 で受信した認証結果が、端末 1 3 に接続許可を与えるものであるか否かを判断し（ステップ S 8）、端末 1 3 に接続許可を与えるものである場合には、接続許可を与える端末 1 3 の端末 ID を情報格納手段 4 9 内の「認証した利用者の端末 ID」テーブルに格納する（ステップ S 9）。これにより、情報
20 格納手段 4 9 には、接続許可を与える（すなわち、認証に成功した）端末 ID 及びユーザ ID が格納される。

- また、認証結果が端末 1 3 に接続許可を与えるものでない場合には、ステップ S 5 で「利用者の認証データ」テーブルに格納された利用者の認証データを削除する（ステップ S 1 0）。そして、認証結果送信手段
25 4 7 は、接続の許可／不許可を示す認証結果を端末 1 3 に対して送信する（ステップ S 1 1）。

一方、認証要求受付手段 4 4 に供給された外部接続検知結果が、外部接続の利用不可能を示すものである場合には、認証要求受付手段 4 4 から認証データ比較手段 4 8 に認証要求が供給される。そして、認証データ比較手段 4 8 は、情報格納手段 4 9 内の「利用者の認証データ」テーブルから当該端末 1 3 の端末 ID に係る認証データを検索し（ステップ S 1 3）、当該端末 ID に係る認証データが存在するか否かを判断する（ステップ S 1 4）。

認証データが存在する場合には、さらに、情報格納手段 4 9 内の「利用者の認証データ」に登録されている認証データと、端末 1 3 から受信した認証データとが一致するか否かを比較し（ステップ S 1 5）、両者が一致するか否かを判断する（ステップ S 1 6）。両者が一致する場合には、認証結果として端末 1 3 の接続許可を設定し（ステップ S 1 7）、両者が一致しなかった場合には、認証結果として端末 1 3 の接続不許可を設定して（ステップ S 1 8）、認証結果送信手段 4 7 に対して認証結果を供給する。また、ステップ S 1 4 で当該端末 ID に係る認証データが見つからなかった場合には、認証結果として端末 1 3 の接続不許可を設定して（ステップ S 1 9）、認証結果送信手段 4 7 に対して認証結果を供給する。そして、認証結果送信手段 4 7 は、接続の許可／不許可を示すこれらの認証結果を端末 1 3 に対して送信する（ステップ S 1 1）。

上記のように、本発明では、端末 1 3 がモバイルルータ下位ネットワーク 4 上の端末アクセス基地局 1 1 に接続する場合（端末 1 3 がモバイルルータ下位ネットワーク 4 に参加する場合）、端末 1 3 は、当該端末 1 3 の端末 ID 及びこの端末 1 3 の利用者とパスワードを含む認証データを認証要求として、本発明で新たにモバイルルータ下位ネットワーク 4 上に配置した下位認証サーバ 1 2 に送信する。

そして、モバイルルータ 1 0 がモバイルルータアクセス基地局 5、6

との接続が利用可能である場合、モバイルルータ下位ネットワーク 4 上
の下位認証サーバ 12 は、ホームネットワーク 2 上の認証サーバ 7 で認
証が行われるよう端末 13 の認証要求をホームネットワーク 2 上の認証
サーバ 7 に送信する。そして、ホームネットワーク 2 の認証サーバ 7 か
5 らの応答である認証結果が認証成功を示すものである場合には、当該端
末 13 に係る認証データを情報格納手段 49 に格納する。下位認証サー
バ 12 は、このようにして格納した認証データを用いて、次回以降の端
末 13 の認証を行うことが可能となる。

これによって、例えば、モバイルルータ 10 及びモバイルルータ下位
10 ネットワーク 4 が高速移動をしている場合など、モバイルルータ 10 と
モバイルルータアクセス基地局 5、6 との接続が切断しやすい状態にあ
る場合、実際にモバイルルータ 10 とモバイルルータアクセス基地局 5、
6 との接続が切断してしまっても、モバイルルータ下位ネットワーク 4
上の下位認証サーバ 12 で認証処理を行うことが可能となる。なお、下
15 位認証サーバ 12 は、当該端末を利用する利用者の認証データや当該端
末 ID を格納している必要がある。したがって、特に、いったん下位認
証サーバ 12 が属するモバイルルータ下位ネットワーク 4 に参加したこ
とのある端末 13 が、例えば、端末アクセス基地局 11 との接続が切れ
てしまい、モバイルルータ下位ネットワーク 4 に再び参加しようとする
20 場合などに有効である。

なお、上記の実施の形態では、モバイルルータ 10 とモバイルルータ
アクセス基地局 5、6 との接続が利用可能か否かに従って、ホームネッ
トワーク 2 に属する認証サーバ 7 で認証を行うか、モバイルルータ下位
ネットワーク 4 に属する下位認証サーバ 12 で認証を行うかを決定して
25 いるが、例えば、全ての端末 13 の認証をまず下位認証サーバ 12 で行
い、認証に失敗した場合のみ、ホームネットワーク 2 に属する認証サー

バ 7 に認証の依頼を行うようにすることも可能である。これによって、
認証に係る時間や認証サーバ 1 2 へのトラフィックを節約することが可能となる。

また、上記の実施の形態では、下位認証サーバ 1 2 は、認証要求のあった
5 所定の端末から認証要求を受けたタイミングで、所定の端末に係る
端末 ID や利用者情報のみを情報格納手段 4 9 に格納しているが、あらかじめ
全ての認証データを情報格納手段 4 9 に格納しておいたり、任意の
タイミングで、下位認証サーバ 1 2 が認証サーバ 7 から認証データを受信
できるようにしたりすることも可能である。

10 以下、図 6 を参照しながら、下位認証サーバ 1 2 が、認証サーバ 7 から、
任意のタイミングで認証データを受信できるよう構成された下位認証
サーバの内部構成について説明する。図 6 は、本発明の実施の形態の
ネットワークに配置されている下位認証サーバの内部構成の別の一例を示す
ブロック図である。なお、図 1 に示されている下位認証サーバ 1 2
15 は、図 6 に示す内部構成を有している。

図 6 に示す下位認証サーバ 1 2 は、ローカル通信手段 6 1、ローカル
通信制御手段 6 2、外部接続検知結果受信手段 6 3、認証要求受付手段
6 4、認証データ比較手段 6 5、認証結果送信手段 6 6、認証情報複製
手段 6 7、情報格納手段 6 8 により構成される。この図 6 に示す内部構
20 成と図 4 に示す内部構成と比較すると、図 6 に示す下位認証サーバ 1 2
は、ホームネットワーク 2 上の認証サーバ 7 における認証結果の処理に係る
手段を有さないことに特徴があることがわかる。

また、図 6 に示す下位認証サーバ 1 2 は、認証情報複製手段 6 7 を有
するという特徴がある。この認証情報複製手段 6 7 は、外部接続検知結
25 果受信手段 6 3 から外部接続検知結果を取得し、外部接続が利用可能状
況に基づいて、ローカル通信制御手段 6 2、ローカル通信手段 6 1、L

AN 30、モバイルルータ 10などを介して、ホームネットワーク 2上の認証サーバ 7から、端末 13の認証に必要な認証データを取得し、取得した認証データを情報格納手段 68に格納することが可能なものである。

- 5 これにより、下位認証サーバ 12は、任意のタイミング（ただし、外部接続が利用可能な場合）で、認証サーバ 7から、認証に必要な認証データを取得することが可能となり、このようにして取得した認証データを参照することによって、ホームネットワーク 2に属する認証サーバ 7と同等の認証能力を発揮できるようになり、認証に係る時間や認証
- 10 サーバ 12へのトラフィックを節約することが可能となる。なお、例えば、下位認証サーバ 12の情報を、ホームネットワーク 2に属する認証サーバ 7が格納する情報と同期させるため、例えば一定周期などの所定のタイミングで、認証サーバ 7から、認証に必要な認証データを複製し、情報格納手段 68内の情報を更新することが好ましい。

15

産業上の利用可能性

- 以上説明したように、本発明によれば、移動体内に配置されている移動ネットワーク（モバイルルータ下位ネットワーク 4）から離れた場所に配置された第 1 認証サーバ（認証サーバ 7）とは別に、第 2 認証サーバ（下位認証サーバ 12）を移動ネットワーク内に配置し、第 2 認証サーバにおいても移動端末（端末 13 a、13 b）の認証が行えるようにするので、移動するモバイルルータと地上側のモバイルルータアクセス
- 20 基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことが可能となる。

25

請 求 の 範 囲

1. 移動体内に配置されている移動ネットワークに移動端末が参加する場合、前記移動ネットワークから離れた場所に配置された第1認証サーバが、前記移動端末の認証を行うことが可能である端末認証システムにおいて、前記移動ネットワーク内に第2認証サーバを配置し、前記第2認証サーバにおいても前記移動端末の認証が行えるよう構成されていることを特徴とする端末認証システム。
- 10 2. 前記第2認証サーバが、前記移動端末の認証を行うことを可能とする認証手段と、前記移動端末の認証時に参照する認証データを格納することが可能な情報格納手段とを有することを特徴とする請求項1に記載の端末認証システム。
- 15 3. 前記移動端末から前記第2認証サーバに対して、認証要求が送信されるよう構成されていることを特徴とする請求項2に記載の端末認証システム。
- 20 4. 前記第2認証サーバが、前記第1認証サーバと前記第2認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記第2認証サーバが前記移動端末から前記認証要求を受けた場合、前記第1認証サーバとの通信が可能と判断された場合には、前記第1認証サーバに前記認証要求を送って前記第1認証サーバから前記移動端末の認証結果を受信し、前記第1認証サーバとの通信が不可能と判断された場合には、
25 前記認証手段を用いて前記移動端末の認証を行うよう構成されていることを特徴とする請求項3に記載の端末認証システム。

5. 前記第 1 認証サーバに前記認証要求を送って前記第 1 認証サーバから前記移動端末の認証結果を受信した場合、前記第 2 認証サーバは、前記移動端末の識別情報と前記移動端末の認証結果とを関連付けて、前記情報格納手段に前記認証データとして格納するよう構成されていることを特徴とする請求項 4 に記載の端末認証システム。

6. 前記第 2 認証サーバが、前記第 1 認証サーバと前記第 2 認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記接続判断手段が前記第 1 認証サーバとの通信が可能か否かを判断し、前記第 1 認証サーバとの通信が可能と判断された場合、前記第 2 認証サーバは、任意のタイミングで前記第 1 認証サーバから前記移動端末の認証に必要な前記認証データを取得し、前記情報格納手段に格納するよう構成されていることを特徴とする請求項 1 に記載の端末認証システム。

15

7. 前記第 2 認証サーバは、所定のタイミングで前記第 1 認証サーバから前記認証データを取得し、前記情報格納手段に格納されている前記認証データを更新するよう構成されていることを特徴とする請求項 6 に記載の端末認証システム。

20

8. 前記第 2 認証サーバで前記移動端末の認証を行って前記移動端末の認証に失敗した場合、前記第 2 認証サーバは、前記第 1 認証サーバに前記認証要求を送って前記第 1 認証サーバから前記移動端末の認証結果を受信するよう構成されていることを特徴とする請求項 3 に記載の端末認証システム。

25

9. 前記第2認証サーバから前記認証要求を送信した前記移動端末に対して、前記第1認証サーバ又は前記第2認証サーバで行われた認証結果が通知されるよう構成されていることを特徴とする請求項3に記載の端末認証システム。

5

10. 移動体内に配置されている移動ネットワークに移動端末が参加する場合、前記移動ネットワークから離れた場所に配置された第1認証サーバが、前記移動端末の認証を行うことが可能である端末認証システムにおける端末認証方法において、前記移動ネットワーク内に配置された第2認証サーバが、前記移動端末の認証を行うことを特徴とする端末認証方法。

10

11. 前記移動端末が、前記第2認証サーバに対して、認証要求を送信することを特徴とする請求項10に記載の端末認証方法。

15

12. 前記第2認証サーバが前記移動端末から前記認証要求を受けた場合、前記第1認証サーバと前記第2認証サーバとの通信が可能か否かを判断し、前記第1認証サーバとの通信が可能と判断された場合には、前記第1認証サーバに前記認証要求を送って前記第1認証サーバから前記移動端末の認証結果を受信し、前記第1認証サーバとの通信が不可能と判断された場合には、前記第2認証サーバが前記移動端末の認証を行うことを特徴とする請求項11に記載の端末認証方法。

20

13. 前記第1認証サーバに前記認証要求を送って前記第1認証サーバから前記移動端末の認証結果を受信した場合、前記第2認証サーバは、前記移動端末の識別情報と前記移動端末の認証結果とを関連付けて格納

25

することを特徴とする請求項 1 2 に記載の端末認証方法。

1 4. 前記第 2 認証サーバが、前記第 1 認証サーバと前記第 2 認証サーバとの通信が可能か否かを判断し、前記第 1 認証サーバとの通信が可能と判断された場合には、任意のタイミングで前記第 1 認証サーバから前記移動端末の認証に必要な前記認証データを取得し格納することを特徴とする請求項 1 1 に記載の端末認証方法。

1 5. 前記第 2 認証サーバが、所定のタイミングで前記第 1 認証サーバから前記認証データを取得し、前記第 2 認証サーバに格納されている前記認証データを更新することを特徴とする請求項 1 4 に記載の端末認証方法。

1 6. 前記第 2 認証サーバで前記移動端末の認証を行って前記移動端末の認証に失敗した場合に、前記第 2 認証サーバから前記第 1 認証サーバに前記認証要求を送り、前記第 1 認証サーバで認証を行い、前記第 1 認証サーバから前記第 2 認証サーバに前記移動端末の認証結果を送信することを特徴とする請求項 1 1 に記載の端末認証方法。

1 7. 前記第 2 認証サーバが、前記認証要求を送信した前記移動端末に対して、前記第 1 認証サーバ又は前記第 2 認証サーバで行われた認証結果を通知することを特徴とする請求項 1 1 に記載の端末認証方法。

1 8. 移動体内に配置されている移動ネットワークに移動端末が参加する場合、前記移動端末の認証を行うことが可能である端末認証サーバにおいて、前記移動ネットワークから離れた場所に配置された端末認証

サーバとは別に、前記移動ネットワーク内に配置されることを特徴とする端末認証サーバ。

19. 前記移動端末の認証を行うことを可能とする認証手段と、前記移動端末の認証時に参照する認証データを格納することが可能な情報格納手段とを有することを特徴とする請求項18に記載の端末認証サーバ。

20. 前記移動端末から認証要求を受信することを特徴とする請求項19に記載の端末認証サーバ。

10

21. 前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記移動端末から前記認証要求を受けた場合、前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能と判断された場合には、前記移動ネットワークから離れた場所に配置された端末認証サーバに前記認証要求を送って、前記移動ネットワークから離れた場所に配置された端末認証サーバから前記移動端末の認証結果を受信し、前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が不可能と判断された場合には、前記認証手段を用いて前記移動端末の認証を行うことを特徴とする請求項20に記載の端末認証サーバ。

22. 前記移動ネットワークから離れた場所に配置された端末認証サーバから前記移動端末の認証結果を受信した場合、前記移動端末の識別情報と前記移動端末の認証結果とを関連付けて、前記情報格納手段に前記認証データとして格納することを特徴とする請求項21に記載の端末認証サーバ。

25

23. 前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能
- 5 と判断された場合、任意のタイミングで、前記移動ネットワークから離れた場所に配置された端末認証サーバから前記移動端末の認証に必要な前記認証データを取得し、前記情報格納手段に格納することを特徴とする請求項18に記載の端末認証サーバ。
- 10 24. 所定のタイミングで、前記移動ネットワークから離れた場所に配置された端末認証サーバから前記認証データを取得し、前記情報格納手段に格納されている前記認証データを更新することを特徴とする請求項23に記載の端末認証サーバ。
- 15 25. 前記認証手段により前記移動端末の認証を行って、前記移動端末の認証に失敗した場合、前記移動ネットワークから離れた場所に配置された端末認証サーバに前記認証要求を送って前記第1認証サーバから前記移動端末の認証結果を受信することを特徴とする請求項19に記載の端末認証サーバ。
- 20 26. 前記認証要求を送信した前記移動端末に対して、前記移動ネットワークから離れた場所に配置された端末認証サーバ、又は、当該端末認証サーバで行われた認証結果を通知することを特徴とする請求項19に記載の端末認証サーバ。

FIG. 1

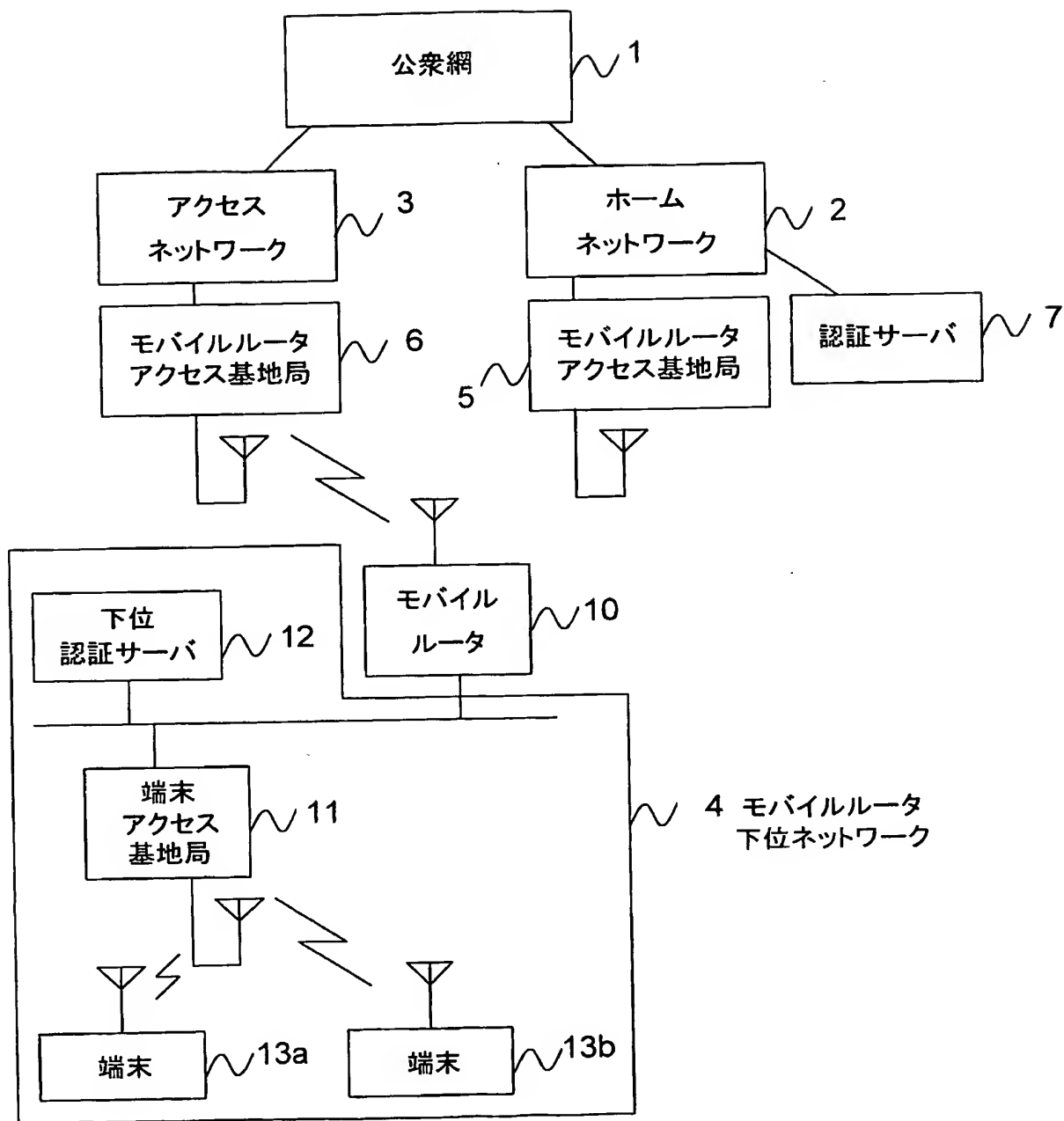


FIG. 2

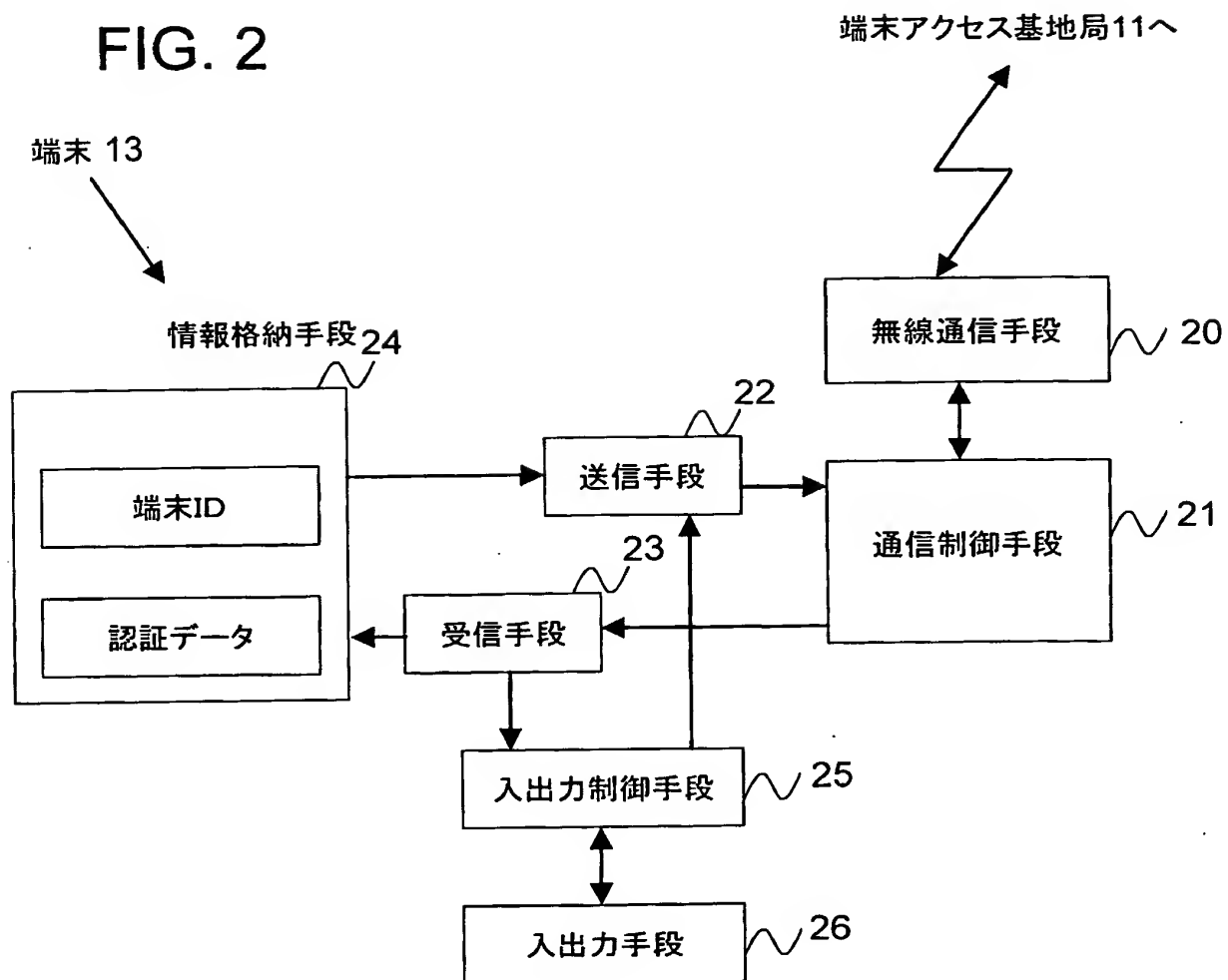


FIG. 3

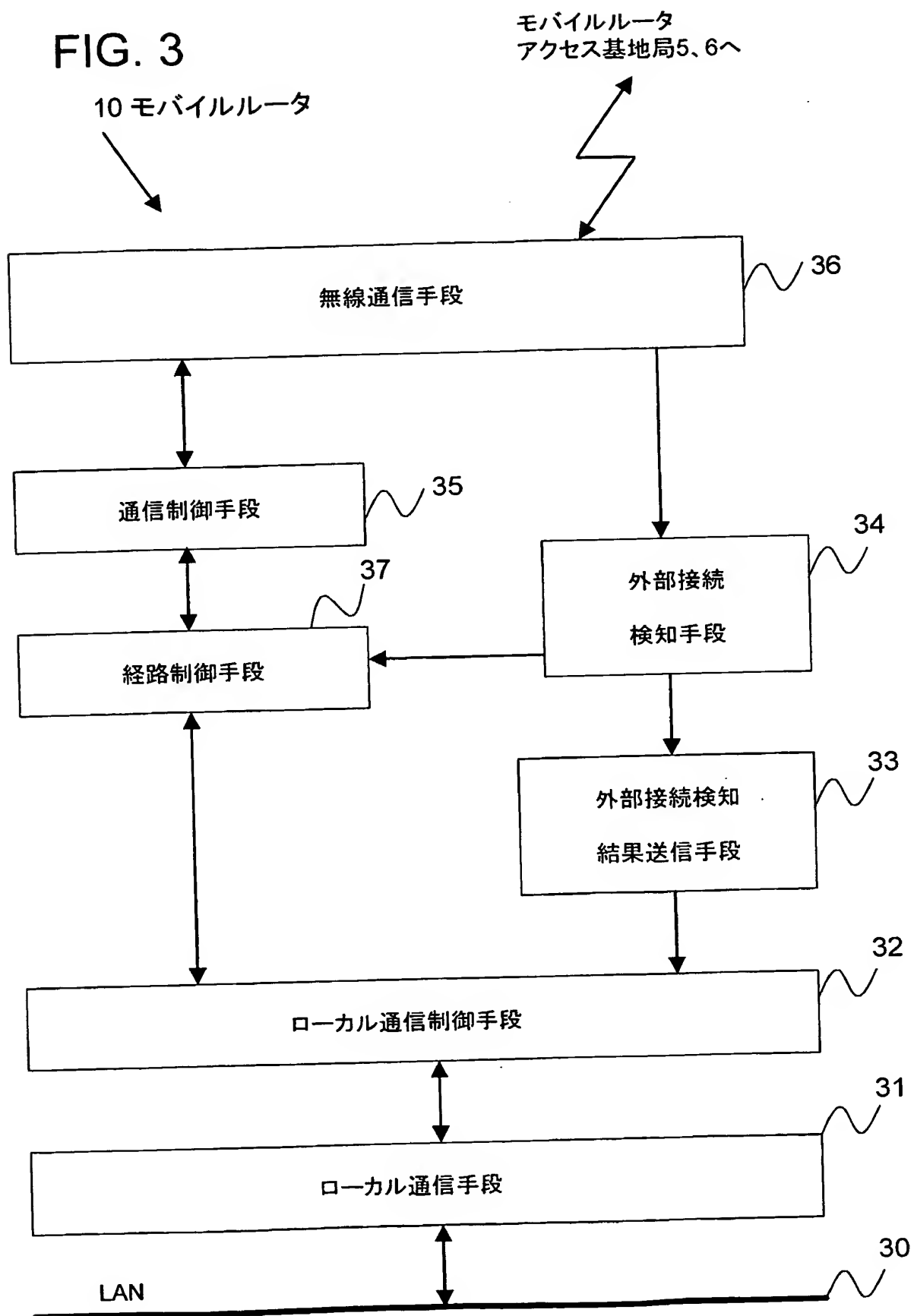
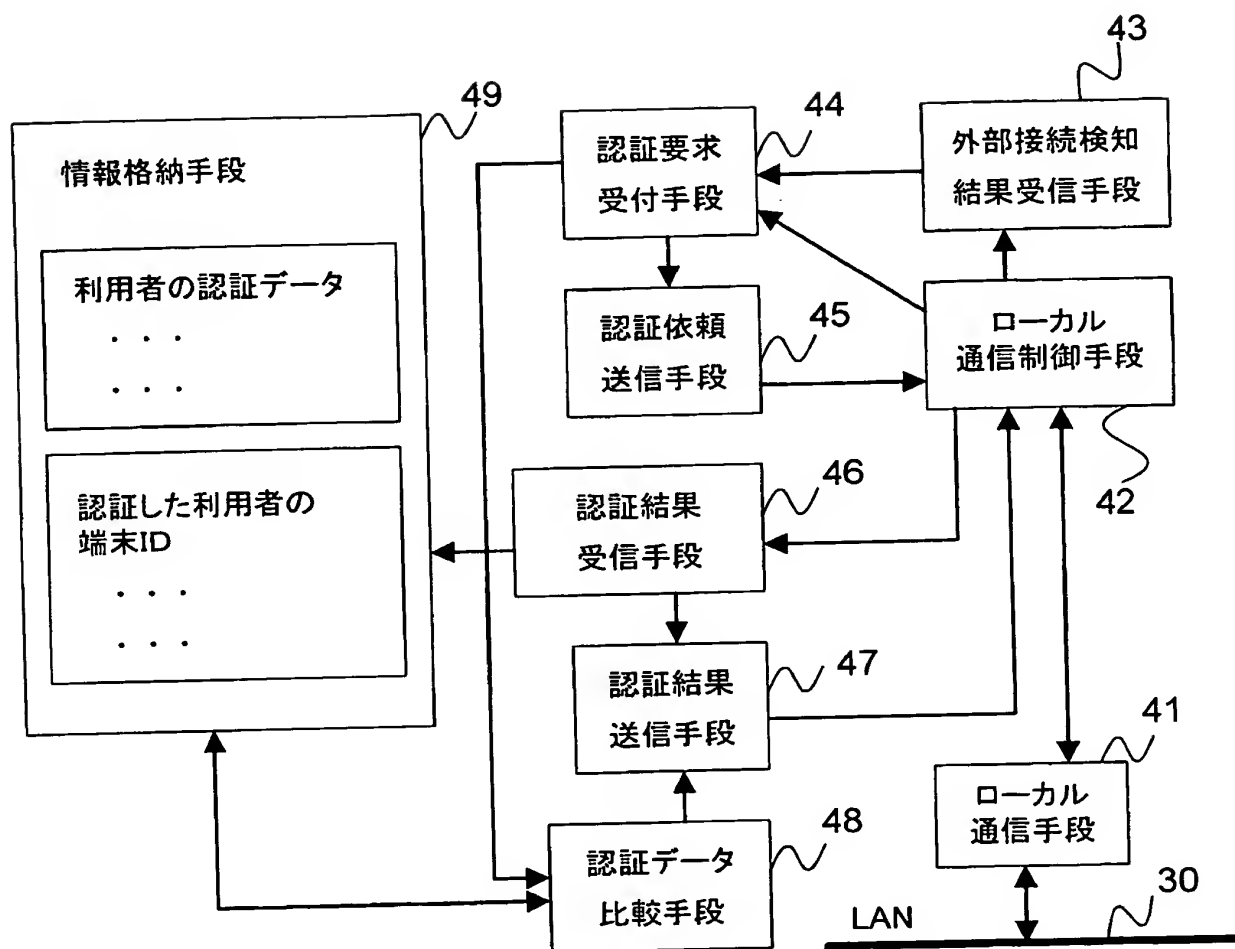


FIG. 4



12 下位認証サーバ

FIG. 5

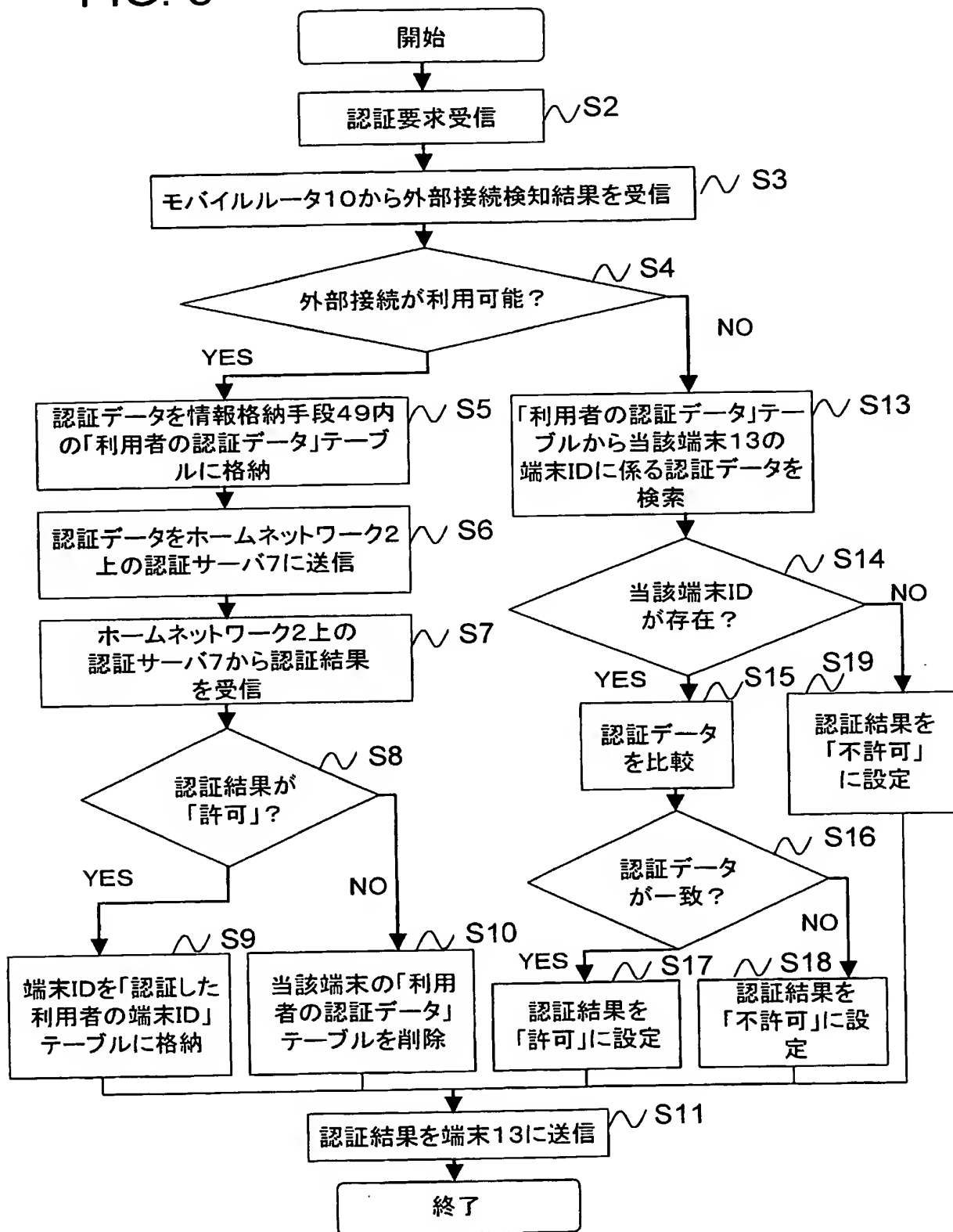


FIG. 6

